What is Claimed Is:

1. A method for enabling identification of at least one address associated with ingress of a packet stream, comprising:

identifying a portion of a packet data communication network as a trusted region;

identifying all border devices at entry points on an outer boundary of the trusted region of the network;

configuring each respective one of the border devices to mark at least predetermined packets transmitted into the trusted region of the network, each marking of a packet by a respective border device comprising providing a fragment of a network address of the respective border device with the packet;

receiving a plurality of marked packets from one of the border devices; and

processing address fragments from the received marked packets to reconstruct the network address of the one border device.

2. The method of claim 1, wherein the configuring step comprises causing each respective border device to mark all packets being transmitted into the trusted region of the network.

3. The method of claim 1, wherein the configuring step comprises causing each respective border device to mark all packets being transmitted to a predetermined destination through a region of the network trusted by the predetermined destination.

4. The method of claim 1, wherein the identified border devices comprise a plurality of routers of one or more autonomous systems of the packet data communication network.

5. The method of claim 4, wherein the packet data communication network is the Internet.

6. The method of claim 4, wherein the plurality of routers include routers on a backbone of one or more autonomous systems.

7. The method of claim 1, wherein each respective one of the configured border devices performs the following steps:

fragmenting an address of the respective border device into a first plurality of overlapping fragments of a first format;

assigning fragment identifiers of a first range to the first fragments;

fragmenting the address of the respective border device into a second plurality of overlapping fragments of a second format;

assigning fragment identifiers of a second range to the second fragments; and

marking a plurality of packets forwarded therefrom into the trusted region by adding the first and second fragments and corresponding assigned identifiers to the plurality of packets forwarded by the respective border device.

8. The method of claim 7, wherein:

the first fragments are formatted to comprise sequential sections of the address of the respective border device having a predetermined number of bits of overlap between consecutive ones of the sequential sections; and

the second fragments are formatted so that each second fragment comprises two offset sections of the address of the respective border device, at least one pair of the second fragments having a predetermined number of bits of overlap.

9. The method of claim 7, wherein the step of processing address fragments from the received marked packets to reconstruct the network address of the one border device comprises:

processing fragments from said plurality of packets forwarded by the border device having identifiers in the first range to compare overlapped bits and combine fragments having matching overlapping bits to a form first copy of the address of the one border device from the first fragments;

processing fragments from said plurality of packets forwarded by the border device having identifiers in the second range to compare overlapped bits and combine fragments having matching overlapping bits to form a second copy of the address of the one border device from the first fragments; and

recognizing a valid reconstructed address if the first and second copies of the address of the one border device match.

10. The method of claim 1, wherein the predetermined packets include packets of a type selected from the group consisting essentially of: packets relating to a denial of service attack; packets containing spam e-mail messages; high volume traffic and packets containing illegally distributed content.

11. The method of claim 1, in combination with at least one step for imposing control on a flow of packets through the one border device whose network address was reconstructed from fragments in received packets.

12. The method of claim 10, wherein the at least one step of imposing control comprises causing the one border device to block transmission into the trusted region of the network of packets addressed to a predetermined destination.

13. The method of claim 1, wherein packet data communication network transports Internet Protocol (IP) type packets comprising headers and data, and each marking of a packet comprises inserting the fragment of the network address of the respective border device into a predetermined field of the IP header of the marked packet

14. The method of claim 13, wherein the predetermined field comprises the Fragmentation Offset field of the IP header.

15. The method of claim 13, wherein the predetermined field comprises the Identification field of the IP header.

16. The method of claim 13, wherein the predetermined field comprises the Fragmentation Offset field and the Identification field of the IP header.

17. The method of claim 16, wherein the fragments comprise IP addresses.

18. A method of marking communication packets forwarded by a router through a packet data communication network with router identifying information, comprising:

fragmenting a network address of the router into a first plurality of overlapping address fragments of a first format;

assigning fragment identifiers of a first range to the first fragments;

fragmenting the network address of the router into a second plurality of overlapping address fragments of a second format;

assigning fragment identifiers of a second range to the second fragments; and

adding the fragments and corresponding assigned identifiers to a plurality of packets forwarded by the router.

19. The method of claim 18, wherein:

the first address fragments are formatted to comprise sequential sections of the network address of the router having a predetermined number of bits of overlap between consecutive ones of the sequential sections; and

the second address fragments are formatted so that each second address fragment comprises two offset sections of the address of the router, at least one pair of the second address fragments having a predetermined number of bits of overlap.

20. The method of claim 18, further comprising forming a hash value from each respective fragment, wherein when each respective fragment is added to a particular packet the hash value formed from the respective fragment is also added to the particular packet.

21. A method of reconstructing an address of a marking device connected at a point on a packet data communication network at or near a source of a flow of packets through the network, comprising:

receiving data packets of the flow containing marks comprising fragments of a network address of the marking device, via the packet data communication network;

for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets, to determine if there is a match; and

for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of the device that marked a plurality of the received packets of the flow.

22. The method of claim 21, wherein the complete address is an Internet Protocol (IP) address of a router on a border of a trusted region of the packet data communication network.

23. The method of claim 22, wherein the packet data communication network is the Internet.

24. The method of claim 23, wherein the complete address identifies an ingress point of the flow of packets representing an attack on at least one target served through the trusted region.

25. The method of claim 23, wherein the complete address identifies an ingress point of a flow of packets containing spam e-mails.

26. The method of claim 23, wherein the complete address identifies an ingress point of a flow of packets containing illegal information content.

27. The method of claim 21, wherein:

the received data packets contain respective fragment identifiers, in first and second ranges;

the matching and concatenation is performed on fragments assigned identifiers in the first range and produces a first version of the complete address;

the method further comprises:

for each respective fragment from a newly received packet containing a fragment identifier in the second range, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets carrying identifiers in the second range, to determine if there is a match; and

for each match between a respective fragment from a newly received packet containing a fragment identifier in the second range and a fragment from a previously received packet

containing a fragment identifier in the second range, concatenating one of the matching fragments with non-matched bits the other one of the matching fragments,

wherein the matching and concatenation for fragments from packets containing fragment identifiers in the second range is performed one or more times until a combination of fragments produces a second version of the complete address of the device that marked a plurality of the received packets.

28. The method of claim 27, further comprising validating the complete address if the first version and the second version match.

29. The method of claim 21, further comprising:

for each received data packet containing a mark, recovering and storing a hash value related to a respective mark from the received data packet containing the respective mark;

upon deriving the complete address, examining stored hash values corresponding to fragments used to derive the complete address; and

identifying the complete address as relating to a source of an attack if at least a predetermined number of hash values corresponding to fragments used to derive the complete address have been received and stored.

30. The method of claim 29, wherein the step of examining comprises:

forming a hash of the complete address;

fragmenting the hash of the complete address; and

comparing the hash fragments to the stored hash values corresponding to fragments used to derive the complete address.

31. A border device for communication through a packet data communication network, comprising:

a communication interface for enabling transmission of packets through the packet data communication network; and

means for marking at least predetermined ones of the packets transmitted through the packet data communication network, wherein marking operations performed by said means comprise:

a) fragmenting a network address of the border device into a first plurality of overlapping fragments of a first format;

b) assigning fragment identifiers of a first range to the first fragments;

c) fragmenting the network address of the border device into a second plurality of overlapping fragments of a second format;

d) assigning fragment identifiers of a second range to the second fragments;

e) adding the fragments and corresponding assigned identifiers to at least the predetermined ones of the packets transmitted through packet data communication network.

32. The border device as in claim 31, wherein the border device is a router, and the means for marking comprise an input port processor in a line card of the router.

33. The border device as in claim 31, wherein the border device is a router, and the means for marking includes a content addressable memory for use in determining if individual packets should be marked.

34. A computer system configured to implement a sequence of steps, to identify a device at or near a point of origin of a particular flow of packets through a packet data communication network, the sequence of steps comprising:

receiving data packets containing marks comprising fragments of a network address of the device, via the packet data communication network;

for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match; and

for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of a device that marked a plurality of the received packets.

35. A computer program product comprising executable code embodied in a machine-readable medium, execution of the code causing a computer to perform a sequence of steps to identify a device at or near a point of origin of a particular flow of packets through the network, the sequence of steps comprising:

receiving data packets containing marks comprising fragments of a network address, via the packet data communication network;

for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match; and

for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of a device that marked a plurality of the received packets.

36. A method of marking communication packets forwarded by a router through a packet data communication network with router identifying information, comprising:

forming one or more first fragments from a first network address associated with the router;

forming one or more second fragments from a second network address associated with the router; and

marking a plurality of packets by adding the fragments to the plurality of packets; and

forwarding the plurality of marked packets from the router through the packet data communication network.

37. The method of claim 36, wherein the first and second addresses are Internet Protocol (IP) addresses of the router.

38. The method of claim 36, wherein at least one of the first and second network addresses is scrambled before the step of forming one or more fragments thereof.

39. The method of claim 36, wherein the first address comprises an Internet Protocol (IP) address of the router and the second address comprises a scrambled IP address of the router.

40. The method of claim 36, wherein:

the first network address is scrambled before the step of forming one or more fragments thereof; and

the second network address is hashed network address is before the step of forming one or more fragments thereof.

41. The method of claim 36, wherein the forming steps produce fragments of one or more Internet Protocol (IP) addresses, fragments of one or more scrambled IP addresses and fragments of one or more hashed IP addresses.